PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-342285**
(43)Date of publication of application : **29.11.2002**

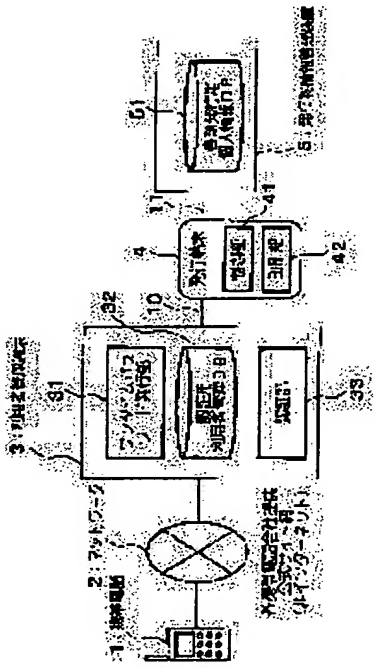
(51)Int.CI. **G06F 15/00**
G06F 17/60
H04L 9/32
H04M 11/00
H04Q 7/38

(21)Application number : **2001-149920**
(22)Date of filing : **18.05.2001**

(71)Applicant : **NTT DATA CORP**
(72)Inventor : **FURUTA SATOSHI**

(54) INFORMATION-ISSUING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an information issuing system, capable of improving security, and easily collecting and issuing necessary information.
SOLUTION: A user management terminal 3 conducts authentication processing, based on authentication information transmitted from a portable telephone; and when the authentication is established, the user management terminal 3 issues an one-time password being information for executing authentication for receiving the permission of the issue of information to the portable telephone. Then, the issues one-time password and the identification information of the portable telephone being the target of the issue of the issued one-time password are stored to be made to correspond to each other; the identification information and one-time password issued from an issuing terminal are received; the authentication processing is executed, based on the temporarily stored information; and when the authentication is established, the issuance of the information is permitted.



LEGAL STATUS

[Date of request for examination] 05.07.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）

公開特許公報（Ａ）

(11)特許出願公開番号
特開2002－342285
（P2002－342285A）

(43)公開日　平成14年11月29日(2002.11.29)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ 15/00	３３０Ｂ	５Ｂ０８５
	17/60	１５４	17/60	１５４	５Ｊ１０４
		３０２		３０２Ｃ	５Ｋ０６７
		５０６		５０６	５Ｋ１０１
		５１２		５１２	

審査請求　有　請求項の数４　ＯＬ　（全８頁）　最終頁に続く

(21)出願番号　特願2001－149920(P2001－149920)

(22)出願日　平成13年５月18日(2001.5.18)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号

(72)発明者　古田　諭
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内

(74)代理人　100064908
弁理士　志賀　正武　（外２名）

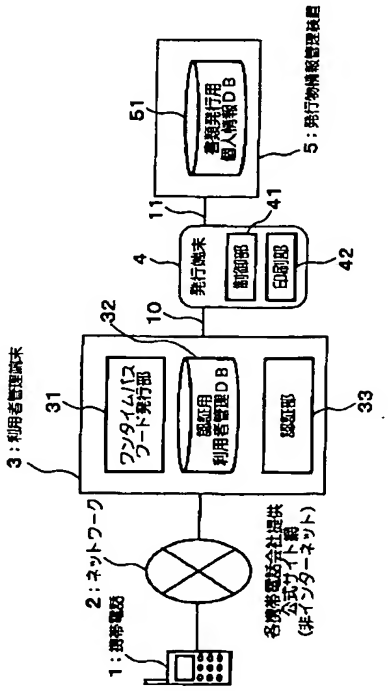
最終頁に続く

(54)【発明の名称】　情報発行システム

(57)【要約】

【課題】　セキュリティを向上させるとともに、必要な情報を簡単に取り寄せて発行することができる情報発行システムを提供する。

【解決手段】　利用者管理端末３は、携帯電話から送信される認証情報に基づいて認証処理を行い、認証が成立した場合に、情報の発行許可を受けるための認証を行う情報であるワンタイムパスワードを携帯電話に発行し、発行されたワンタイムパスワードと該発行されたワンタイムパスワードの発行対象の携帯電話の識別情報とを対応づけて一時記憶し、発行端末から送信される識別情報とワンタイムパスワードとを受信し、一時記憶された情報に基づいて認証処理を行い、認証が成立した場合に情報の発行を許可する。



【特許請求の範囲】
【請求項１】　携帯電話から送信される情報の発行要求を受信する利用者管理端末と、該利用者管理端末からの指示に基づいて、前記携帯電話から発行要求された情報をデータベースから読み出して発行する発行端末とが接続される情報発行システムであって、
前記利用者管理端末は、前記携帯電話を認証するための情報である認証情報と前記携帯電話から送信される携帯電話を識別するための情報である識別情報とを記憶する第１の記憶手段と、前記携帯電話から送信される認証情報と識別情報とを前記第１の記憶手段に記憶された情報に基づいて認証処理を行う第１の認証手段と、前記第１の認証手段の認証処理において認証が成立した場合に、情報の発行許可を受けるための認証を行う情報であるワンタイムパスワードを発行して前記携帯電話に送信するワンタイムパスワード発行手段と、前記ワンタイムパスワード発行手段によって発行されたワンタイムパスワードと該発行されたワンタイムパスワードの発行対象の携帯電話の識別情報１とを対応づけて記憶する第２の記憶手段と、前記発行端末から送信される識別情報とワンタイムパスワードとを受信して前記第２の記憶手段に記憶されている情報に基づいて認証処理を行う第２の認証手段と、前記第２の認証手段の認証処理において認証が成立した場合に情報の発行を許可する発行許可情報を前記発行端末に送信する制御を行う発行許可制御手段とを有し、
前記発行端末は、携帯電話から送信される識別情報とワンタイムパスワードとを受信し、該受信した識別情報とワンタイムパスワードとを利用者管理端末に送信する制御を行う第１の制御手段と、前記利用者管理端末から発行許可情報を受信した場合に、発行対象となる情報を前記データベースから読み出して発行する発行手段とを有することを特徴とする情報発行システム。
【請求項２】　携帯電話から送信される情報の発行要求を受信する利用者管理端末と、該利用者管理端末からの指示に基づいて、前記携帯電話から発行要求された情報をデータベースから読み出して発行する発行端末とが接続される情報発行システムに用いられる利用者管理端末であって、
前記携帯電話を認証するための情報である認証情報と前記携帯電話から送信される携帯電話を識別するための情報である識別情報とを記憶する第１の記憶手段と、
前記携帯電話から送信される認証情報と識別情報とを前記第１の記憶手段に記憶された情報に基づいて認証処理を行う第１の認証手段と、
前記第１の認証手段の認証処理において認証が成立した場合に、情報の発行許可を受けるための認証を行う情報であるワンタイムパスワードを発行して前記携帯電話に送信するワンタイムパスワード発行手段と、
前記ワンタイムパスワード発行手段によって発行されたワンタイムパスワードと発行されたワンタイムパスワードの発行対象の携帯電話の識別情報とを対応づけて記憶する第２の記憶手段と、
前記発行端末から送信される識別情報とワンタイムパスワードとを受信して前記第２の記憶手段に記憶されている情報に基づいて認証処理を行う第２の認証手段と、
前記第２の認証手段の認証処理において認証が成立した場合に情報の発行を許可する発行許可情報を前記発行端末に送信する制御を行う発行許可制御手段と、を有することを特徴とする利用者管理端末。
【請求項３】　前記ワンタイムパスワード発行手段は、発行毎に異なるワンタイムパスワードを発行することを特徴とする請求項２記載の利用者管理端末。
【請求項４】　携帯電話から送信される情報の発行要求を受信する利用者管理端末と、該利用者管理端末からの指示に基づいて、前記携帯電話から発行要求された情報をデータベースから読み出して発行する発行端末とが接続される情報発行システムに用いられる発行端末であって、
携帯電話から送信される識別情報とワンタイムパスワードとを受信し、該受信した識別情報とワンタイムパスワードとを利用者管理端末に送信する制御を行う制御手段と、
前記利用者管理端末から発行許可情報を受信した場合に、発行対象となる情報を前記データベースから読み出して発行する発行手段と、
を有することを特徴とする発行端末。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、携帯電話から発行が要求された情報を発行する情報発行システムに関するものである。
【０００２】
【従来の技術】従来より、住民票や印鑑証明などの公的証明書が必要になった場合に、利用者は、区役所等の行政機関に出向き、必要な書類を発行してもらっている。しかし、この行政機関に出向いて必要書類を発行してもらう方法によれば、休みあるいは受け付け時間外等により行政機関が書類発行の取り扱いを行っていない場合、利用者は、即時に書類を発行してもらうことができなかった。そこで、役所、省庁などの行政機関に設けられ、発行する書類に関するデータを管理するデータベースを利用し、インターネットを介して書類の発行を行う書類発行端末を接続して書類発行を行うシステムを構築する。そして、この書類発行端末を、駅などの複数の利用者が利用可能な場所に設置し、書類発行のサービスを提供することが考えられる。
【０００３】
【発明が解決しようとする課題】しかしながら、上述した書類を発行するシステムにおいては、書類発行端末を

操作することによって書類を発行すことができるが、悪意ある第３者によって発行端末が操作されて書類が発行され、書類が悪用されてしまう可能性があった。本発明は、このような事情に鑑みてなされたもので、その目的は、セキュリティを向上させるとともに、必要な情報を簡単に取り寄せて発行することができる情報発行システムを提供することにある。

【０００４】

【課題を解決するための手段】上記目的を達成するために、本発明は、携帯電話（例えば、実施の形態における携帯電話１）から送信される情報（例えば、実施の形態における住民票、印鑑証明書などの公的証明書や有償チケットなど）の発行要求を受信する利用者管理端末（例えば、実施の形態における利用者管理端末３）と、該利用者管理端末からの指示に基づいて、前記携帯電話から発行要求された情報をデータベース（例えば、実施の形態における書類発行用個人情報データベース５１）から読み出して発行する発行端末（例えば、実施の形態における発行端末４）とが接続される情報発行システム（例えば、実施の形態における情報発行システム）であって、前記利用者管理端末は、前記携帯電話を認証するための情報である認証情報（例えば、実施の形態におけるユーザＩＤとパスワード）と前記携帯電話から送信される携帯電話を識別するための情報である識別情報（例えば、実施の形態における電話番号、個別ＩＤ）とを記憶する第１の記憶手段（例えば、実施の形態における認証用利用者管理データベース３２）と、前記携帯電話から送信される認証情報と識別情報とを前記第１の記憶手段に記憶された情報に基づいて認証処理を行う第１の認証手段（例えば、実施の形態における認証部３３）と、前記第１の認証手段の認証処理において認証が成立した場合に、情報の発行許可を受けるための認証を行う情報であるワンタイムパスワードを発行して前記携帯電話に送信するワンタイムパスワード発行手段（例えば、実施の形態におけるワンタイムパスワード発行部３１）と、前記ワンタイムパスワード発行手段によって発行されたワンタイムパスワードと該発行されたワンタイムパスワードの発行対象の携帯電話の識別情報（例えば、実施の形態における個別ＩＤ）とを対応づけて記憶する第２の記憶手段（例えば、実施の形態における認証用利用者管理データベース３２）と、前記発行端末から送信される識別情報とワンタイムパスワードとを受信して前記第２の記憶手段に記憶されている情報に基づいて認証処理を行う第２の認証手段（例えば、実施の形態における認証部３３）と、前記第２の認証手段の認証処理において認証が成立した場合に情報の発行を許可する発行許可情報を前記発行端末に送信する制御を行う発行許可制御手段（例えば、実施の形態における認証部３３）とを有し、前記発行端末は、携帯電話から送信される識別情報とワンタイムパスワードとを受信し、該受信した識別情報とワンタイムパスワードと利用者管理端末に送信する制御を行う第１の制御手段（例えば、実施の形態における制御部４１）と、前記利用者管理端末から発行許可情報を受信した場合に、発行対象となる情報を前記データベースから読み出して発行する発行手段（例えば、実施の形態における印刷部４２）とを有することを特徴とする。

【０００５】また、本発明は、携帯電話から送信される情報の発行要求を受信する利用者管理端末と、該利用者管理端末からの指示に基づいて、前記携帯電話から発行要求された情報をデータベースから読み出して発行する発行端末とが接続される情報発行システムに用いられる利用者管理端末であって、前記携帯電話を認証するための情報である認証情報と前記携帯電話から送信される携帯電話を識別するための情報である識別情報とを記憶する第１の記憶手段と、前記携帯電話から送信される認証情報と識別情報とを前記第１の記憶手段に記憶された情報に基づいて認証処理を行う第１の認証手段と、前記第１の認証手段の認証処理において認証が成立した場合に、情報の発行許可を受けるための認証を行う情報であるワンタイムパスワードを発行して前記携帯電話に送信するワンタイムパスワード発行手段と、前記ワンタイムパスワード発行手段によって発行されたワンタイムパスワードと該発行されたワンタイムパスワードの発行対象の携帯電話の識別情報とを対応づけて記憶する第２の記憶手段と、前記発行端末から送信される識別情報とワンタイムパスワードとを受信して前記第２の記憶手段に記憶されている情報に基づいて認証処理を行う第２の認証手段と、前記第２の認証手段の認証処理において認証が成立した場合に情報の発行を許可する発行許可情報を前記発行端末に送信する制御を行う発行許可制御手段と、を有することを特徴とする。

【０００６】また、本発明は、上述の利用者管理端末において、前記ワンタイムパスワード発行手段は、発行毎に異なるワンタイムパスワードを発行することを特徴とする。

【０００７】また、本発明によれば、携帯電話から送信される情報の発行要求を受信する利用者管理端末と、該利用者管理端末からの指示に基づいて、前記携帯電話から発行要求された情報をデータベースから読み出して発行する発行端末とが接続される情報発行システムに用いられる発行端末であって、携帯電話から送信される識別情報とワンタイムパスワードとを受信し、該受信した識別情報とワンタイムパスワードとを利用者管理端末に送信する制御を行う制御手段と、前記利用者管理端末から発行許可情報を受信した場合に、発行対象となる情報を前記データベースから読み出して発行する発行手段と、を有することを特徴とする。

【０００８】

【発明の実施の形態】以下、本発明の一実施形態による

情報発行システムを図面を参照して[redacted]する。図１は、この発明の一実施形態による情報発行[redacted]ステムの構成を示す概略ブロック図である。携帯電話１は、無線によってネットワーク２を介して利用者管理センタに設けられる認証用利用者管理データベース３２に接続される。この携帯電話１には、携帯電話１を識別するための個別ＩＤが予め設定されている。なお、携帯電話１は、ディジタル簡易電話システムの端末であってもよい。ネットワーク２は、例えば、携帯電話１の通信サービスを提供する通信業者によって提供される公式サイト網である。ここでは、ネットワーク２としてインターネット以外のネットワークが用いられる。

【０００９】利用者管理装置３は、ワンタイムパスワード発行部３１と、認証用利用者管理データベース３２と、認証部３３とを有し、ネットワーク１０を介して発行端末４に接続され、書類発行許可情報を発行端末４に送信する機能を有する。ワンタイムパスワード発行部３１は、携帯電話１からの指示に応じて、ワンタイムパスワードを携帯電話１に発行する。ここでいうワンタイムパスワードとは、書類の発行許可を受けるための認証を行う情報であり、発行する毎に異なるワンタイムパスワードが発行される。また、発行されたワンタイムパスワードは、発行先のユーザＩＤ（あるいは個別ＩＤ）に対応づけられ認証用利用者管理データベース３に記憶される。

【００１０】認証用利用者管理データベース３２は、携帯電話１の利用者を認証するための利用者管理情報を記憶する。この認証用利用者管理データベース３に記憶される利用者管理情報の一例を図２に示す。図２に示すように、利用者管理情報には、利用者の認証を行うためのユーザＩＤにパスワード、利用者の住所、氏名、電話番号等、各利用者の個人の情報である個人情報、個別ＩＤ、携帯電話１の電子メールアドレス、発行したログの管理や発行した書類の管理をして証明書の真偽を確認する為に使用される情報である識別ＩＤ、ワンタイムパスワード発行部３１によって発行されたワンタイムパスワードなど、が対応づけられ、記憶される。この認証用利用者管理データベース３２が、上述の第１の記憶手段および第２の記憶手段に相当する。

【００１１】認証部３３は、携帯電話１から認証要求を受信すると、認証用利用者管理データベース３２に記憶されている情報に基づいて、認証要求に含まれているパスワードと個別ＩＤとがユーザＩＤに対応しているか否かを検出し、認証を行う。また、認証部３３は、発行端末４から送信されるワンタイムパスワードを受信して認証用利用者管理データベース３２に記憶されている利用者管理情報に基づいて認証処理を行う。さらに、認証部３３は、情報の発行を許可する発行許可情報を発行端末４に発行する制御を行う。この認証部３３が、上述の第１の認証手段と第２の認証手段と発行許可制御手段とに相当する。

【００１２】発行端末４は、制御部４１と印刷部４２とを有し、例えば、コンビニエンスストア、駅、百貨店等に設けられる。この制御部４１は、携帯電話１から送信される携帯電話１を識別する識別情報（例えば、電話番号、個別ＩＤなどのユーザが簡単に変更できない情報）とワンタイムパスワードとを受信し、受信した識別情報とワンタイムパスワードを利用者管理端末３に送信する制御を行う。また、制御部４１は、利用者管理端末３から書類発行許可情報を受信した場合に、受信した書類発行許可情報を発行物情報管理装置５に送信する制御を行う。書類発行許可情報とは、発行物情報管理装置５に記憶されている情報を発行端末４に送信し、発行端末４による発行物の発行を許可する情報である。また、制御部４１は、発行物を指定する情報が入力部を介して入力された場合に、発行物を指定する情報を発行物情報管理装置５に送信する。ここで、発行物を指定する情報とは、発行物情報管理装置５に記憶されている情報を指定して発行物を発行させるための情報である。

【００１３】印刷部４２は、制御部４１からの指示に応じて印刷物の印刷を行う。また、発行端末４は、各種情報を表示するＣＲＴ（Ｃａｔｈｏｄｅ　ＲａｙＴｕｂｅ）または液晶表示装置等の表示部と、キーボード、マウス等の入力部と、発行物を指定する情報に基づいて料金を算出し投入部から投入される料金の精算を行う課金部とを有する。なお、この表示部と入力部とをタッチパネルなどで構成するようにしてもよい。

【００１４】発行物情報管理装置５は、書類発行用個人情報データベース５１を有し、専用線１１によって発行端末４に接続される。書類発行用個人情報データベース５１は、利用者個人に関する情報を記憶している。利用者個人に関する情報とは、例えば、利用者の住所、氏名等の個人の情報と、これら個人の情報に基づいて住民票や印鑑証明等の書類を作成して発行するための情報とが含まれる。発行物情報管理装置５は、発行端末４から発行物を指定する情報を受信した場合に、受信した発行物を指定する情報に対応する利用者個人に関する情報を書類発行用個人情報データベース５１から読み出し、発行データとして発行端末４に専用線１１を介して送信する。また、発行物情報管理装置５は、発行端末４からの要求に応じて、識別ＩＤを発行する機能を有する。

【００１５】次に、上述した構成における情報発行システムの動作を図面を用いて説明する。図３は、図１の構成における情報発行システムの動作を説明するための説明図である。ここでは、発行物として、住民票を発行する場合について説明する。また、ここでは、携帯電話１の利用者が発行端末４の電子メールアドレスを把握しているあるいは、携帯電話１に発行端末４の電子メールアドレスが記憶されているものとする。まず、利用者は、携帯電話１を携帯し、発行端末４が設置されている場所

に出向く。そして、携帯電話１の入[redacted]ーを操作し、ネットワーク２（公式サイト網）を介[redacted]、利用者管理端末３との通信を確立するための認証用のホームページにアクセスする。そして、このホームページの入力フォーマットに従って、ユーザＩＤとパスワードとを含む認証要求を入力し、ネットワーク２を介して利用者管理端末３に送信する。このとき、認証要求には、送信元を示す携帯電話１の個別ＩＤがさらに付加されて送信される（ステップＳ１）。

【００１６】利用者管理端末３は、携帯電話１から認証要求を受信すると、認証用利用者管理データベース３２に記憶されている情報に基づいて、認証部３３によって、受信した認証要求に含まれているパスワードと個別ＩＤとがユーザＩＤに対応しているか否かを検出し、認証処理を行う（ステップＳ２）。認証処理において、パスワードと個別ＩＤとがユーザＩＤに対応していない場合、利用者管理端末３は、携帯電話１にエラーを送信する。

【００１７】一方、認証処理において、パスワードと個別ＩＤとがユーザＩＤに対応している場合、利用者管理端末３は、ワンタイムパスワード発行部３１によってワンタイムパスワードを発行し、発行したワンタイムパスワードを携帯電話１のユーザＩＤに対応づけて認証用利用者管理データベース３２に記憶するとともに、携帯電話１に送信する（ステップＳ３）。このワンタイムパスワードの送信は、認証されたユーザＩＤとパスワードに対応づけて認証用利用者管理データベース３２に記憶されている電子メールアドレスが送信先として設定されて送信される。

【００１８】携帯電話１は、利用者管理端末３からワンタイムパスワードを受信すると、ワンタイムパスワードを受信したことを表示画面に表示する。このとき、ワンタイムパスワードそのものは、表示画面に表示されない。利用者は、ワンタイムパスワードを受信したことを確認した後、送信元として携帯電話１の電子メールアドレスが設定されたワンタイムパスワードと個別ＩＤとを電子メールを発行端末４に転送する（ステップＳ４）。

【００１９】発行端末４は、制御部４１によって携帯電話１から受信したワンタイムパスワードと個別ＩＤとを含む電子メールを利用者管理端末３に送信し、ワンタイムパスワードが正しいか否かを問い合わせ、認証依頼をする（ステップＳ５）。利用者管理端末３は、発行端末４から送信される電子メールを受信すると、認証用利用者管理データベース３２に記憶されている情報に基づいて、電子メールに含まれる携帯電話１のワンタイムパスワードと個別ＩＤとが対応しているか否かを認証部３３によって検出し、認証する（ステップＳ６）。認証処理において、ワンタイムパスワードと個別ＩＤとのうち、どちらか一方でも一致しない場合、エラーとなる。

【００２０】一方、認証処理において、ワンタイムパスワードと個別ＩＤとが[redacted]場合、利用者管理端末３は、このワンタイムパス[redacted]ドと個別ＩＤとが一致した利用者の個人情報の一部（例えば、住所と氏名）とを認証用利用者管理データベース３２から読みだし、読み出した個人情報の一部と書類発行許可情報とを発行端末４に送信する（ステップＳ７）。

【００２１】発行端末４は、利用者管理端末３から個人情報の一部と書類発行許可情報を受信すると、表示部に必要書類を選択するためのサービス選択画面の表示を行う。そして、利用者によって、サービス選択画面の中から「住民票」の項目が指定され、「住民票」を発行する料金が発行端末４に投入されると（ステップＳ８）、発行端末４の制御部４１は、「住民票」を指定する情報と個人情報の一部と識別ＩＤを発行させるためのコマンドとを発行物情報管理装置５に専用線１１を介して送信する（ステップＳ９）。

【００２２】発行物情報管理装置５は、発行端末４から「住民票」を指定する情報と個人情報の一部と識別ＩＤを発行させるためのコマンドとを受信すると、「住民票」を指定する情報と個人情報の一部とに対応する利用者個人に関する情報を読み出し、読み出した利用者個人に関する情報に基づいて住民票を発行するための発行データを生成する。そして、発行物情報管理装置５は、識別ＩＤを発行し、発行した識別ＩＤと発行データとを発行端末４に送信する（ステップＳ１０）。さらに、発行物情報管理装置５は、識別ＩＤを書類発行用個人情報データベース５１に記憶するとともに、利用者管理端末３に識別ＩＤ個人情報の一部とを通知する。発行端末４は、発行物情報管理装置５から送信される発行データ受信すると、受信した発行データに基づき、印刷部４２によって住民票を印刷し、発行する（ステップＳ１１）。利用者管理端末３は、発行物情報管理装置５から送信された個人情報の一部に対応するユーザＩＤに関連づけて、通知された識別ＩＤを認証用利用者管理データベース３２に記憶する。

【００２３】以上説明した実施形態によれば、ステップＳ３において、ワンタイムパスワードを送信する場合に、ワンタイムパスワードの送信先の電子メールアドレスを利用者に入力させるのではなく、ステップＳ１において送信されるユーザＩＤとパスワードに対応する電子メールアドレスを認証用利用者管理データベース３２から読み出し、読み出した電子メールアドレスを送信先としてワンタイムパスワードを送信するようにした。これにより、携帯電話１以外（例えば、パーソナルコンピュータ）からのアクセスを防止するとともに、ワンタイムパスワードを発行先である携帯電話１に確実に送信することができる。

【００２４】また、上述の実施形態によれば、発行端末４と発行物情報管理装置５とを専用線１１を介して接続するようにしたので、外部からの不正な侵入を低減させ

ることができる。また、上述の実施形態によれば、ネットワーク２に公式サイト網を適用することにより、携帯電話１の個別ＩＤに基づいて、アクセスしてきた携帯電話１の判別を容易に行うことができる。すなわち、公式サイト網を利用することにより、携帯電話１の通信サービス契約時に通信業者によって利用者が認証された後に付与される個別ＩＤが電子メールの送信時に利用者管理端末３に通知されるため、アクセスしてきた携帯電話１の所有者等の人物を特定することができる。また、特定の端末からのアクセスのみ受け付けるように制限することができ、これにより、パーソナルコンピュータ等に比べて機能が限られた携帯電話からしかアクセスする事ができない。従って、公式サイト網を利用することにより、ハッキング等の不正行為を低減させることができる。

【００２５】また、上述の実施形態によれば、情報発行システム側において、人手を介さずに発行処理を行うことができ、利用時間に制限を持たせることなく、２４時間対応のシステムの実現が可能であり、行政サービスの向上を図ることができる。また、上述の実施形態によれば、発行端末４が置いてある場所（コンビニエンスストアや駅など）一ヶ所に行くだけで複数の自治体から発行される公的書類もすべて手にすることも可能である。

【００２６】利用者本人が発行端末４の側で発行操作を行うことにより、発行された印刷物をすぐに受け取ることができるとともに、第３者を介さずに印刷物を受け取ることができるので、発行された印刷物を利用者が受け取る前に盗難される場合を低減させることができる。

【００２７】なお、以上説明した実施形態において、ワンタイムパスワードに有効期限を設けておき、有効期限が経過したワンタイムパスワードを認証用利用者管理データベース３上から削除するようにしてもよい。これにより、ワンタイムパスワードが悪用され不正なアクセスがなされることを低減させることができる。また、発行物の真偽を確認する必要がある場合は、真偽を確認する対象となる発行物が発行物情報管理装置５において発行されたか否かについて、書類発行用個人情報データベース５１に識別ＩＤが記録されているか否かを確認することによって行われる。これにより、発行物の偽造などを発見することに利用でき、セキュリティの向上を図ることができる。また、利用者管理端末３の認証用利用者管理データベース３２に記憶されている識別ＩＤを利用して、発行物の真偽を確認するようにしてもよい。

【００２８】また、上述の実施形態においては、発行端末４によって公的証明書（住民票）を発行する場合について説明したが、発行端末４が発行する発行物は、公的証明書に限られるものではない。すなわち、書類発行用個人情報データベース５１に記憶される情報は、利用者個人に関する情報に限られるものではなく、利用者に提供可能な情報であればよい。例えば、画像や、航空チケット、コンサートチケットの有償チケット等の情報等がある。

【００２９】また、上述した実施形態において、携帯電話１から発行端末４にワンタイムパスワードを送信する場合に、電子メールを利用した場合について説明したが、ワンタイムパスワードを送信することができるものであれば、電子メール以外を用いるようにしてもよい。例えば、近距離無線通信（赤外線、ＢＬＵＥＴＯＯＴＨ等）を利用してワンタイムパスワードを送信するようにしてもよい。また、携帯電話１と発行端末４とを接続コネクタ等を用いてワンタイムパスワードを送信するようにしてもよい。

【００３０】また、上述した実施形態において、携帯電話１として、例えば、パームトップ・コンピュータ、ウエアラブル・コンピュータ等の携帯情報端末を適用するようにしてもよい。また、携帯情報端末または携帯電話１にユーザの情報が記録可能かつ取り外し可能なＩＣチップ等の記録媒体が搭載される場合、この記録媒体を携帯情報端末あるいは携帯電話１から取り出し、発行端末４に接続し、発行端末４によってこの記録媒体に記憶されたユーザの情報を読み出して認証を行った後、ワンタイムパスワード発行処理を行うようにしてもよい。

【００３１】また、上述の実施形態において、利用者管理端末３においてパスワード等の認証する場合において、複数回（例えば、３回）の認証失敗で該当ユーザＩＤをロックする機能を設け、携帯電話１の盗難・窃盗による不正使用を防止するようにしてもよい。

【００３２】また、図１におけるワンタイムパスワード発行部３１、認証部３３、制御部４１、印刷部４２の機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより情報の発行管理を行ってもよい。なお、ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものとする。

【００３３】また、「コンピュータシステム」は、ＷＷＷシステムを利用している場合であれば、ホームページ提供環境（あるいは表示環境）も含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムを送信する場合の通信線のように、短時間の間、動的にプログラムを保持するもの、その場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリのように、一定時間プログラムを保持しているものも含むものとする。また上記プログラムは、前述した機能の一部を実現するためのものであっても良

く、さらに前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるものであっても良い。

【００３４】以上、この発明の実施形態を図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

【００３５】

【発明の効果】以上説明したように、この発明によれば、携帯電話から送信される認証情報と識別情報とに基づいて認証処理を行い、認証が成立した場合に、情報の発行許可を受けるための認証を行う情報であるワンタイムパスワードを携帯電話に発行し、発行されたワンタイムパスワードと該発行されたワンタイムパスワードの発行対象の携帯電話の識別情報とを対応づけて一時記憶し、発行端末から送信される識別情報とワンタイムパスワードとを受信し、一時記憶された情報に基づいて認証処理を行い、認証が成立した場合に情報の発行を許可するようにした。これにより、セキュリティを向上させるとともに、必要な情報を簡単に取り寄せて発行することができる。

【００３６】利用者は、情報の発行依頼を行う場合に、携帯電話から発行依頼を行うことができるので、コンピュータを利用する場合に比べて簡単に情報の発行を行うことができる。また、この発明によれば、発行毎に異なるワンタイムパスワードを発行するようにしたので、さらにセキュリティを向上させることができる効果が得られる。

【００３７】また、発行された証明書に対して識別ＩＤを設けるようにしたので、発行された証明書の真偽を識別ＩＤを利用して確認することも可能であり、セキュリティの向上を図ることができる効果が得られる。

【図面の簡単な説明】

【図１】　この発明の一実施形態による情報発行システムの構成を示す概略ブロック図である。

【図２】　認証用利用者管理データベース３に記憶される利用者管理情報を説明するための図面である。

【図３】　図１の構成における情報発行システムの動作を説明するための説明図である。

【符号の説明】

１　携帯電話　　３　利用者管理端末

４　発行端末　　５　発行物情報管理装置

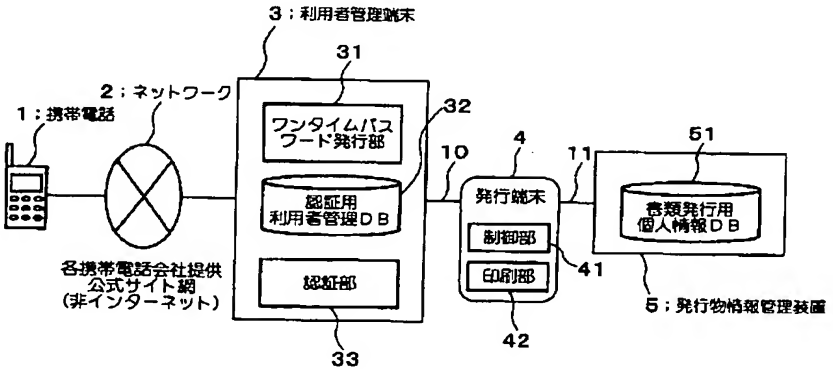
３１　ワンタイムパスワード発行部

３２　認証用利用者管理データベース

３３　認証部　　４１　制御部

４２　印刷部　　５１　書類発行用個人情報データベース

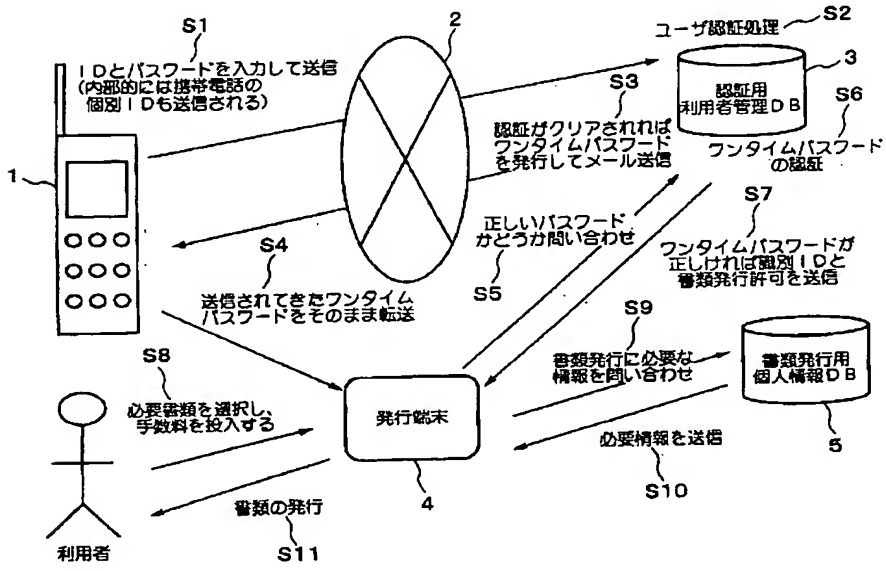
【図１】



【図２】

ユーザＩＤ	パスワード	個人情報	個別ＩＤ	メールアドレス	識別ＩＤ	ワンタイムパスワード
ＵＩＤ001	12345678	東京都…,○○一郎	ABC0001	XX@△△.com	XYZ748	951183121

【図３】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		テーマコード(参考)
Ｈ０４Ｌ 9/32		Ｈ０４Ｍ 11/00	３０２	
Ｈ０４Ｍ 11/00	３０２	Ｈ０４Ｂ 7/26	１０９Ｓ	
Ｈ０４Ｑ 7/38		Ｈ０４Ｌ 9/00	６７３Ａ	

Ｆターム(参考) 5B085 AA08 AE01 BA07 BE07 BG04
BG07
5J104 AA07 KA01 KA21 NA05 PA02
PA07
5K067 AA21 BB04 BB21 DD17 DD23
EE02 EE10 HH22 HH23 HH24
5K101 LL12 MM07 NN21 PP04